Steganography in Mobile Phones on Multimedia Data

Prof. Samir B. Patel, Mr. Vivek R. Vekariya and Mr. Mitesh K. Pithadiya

Abstract -- Mobile camera was developed so that people do not have to carry any separate gadgets with them all the time, since it is integrated with their mobile phones; it helps in capturing images whenever and wherever wanted. But this mobile camera is also used for some wicked purposes i.e. nude photography followed by harassment to the individual. Hence there is an utmost need to prevent such type of happenings. We have tried to developed a module which will run when the image is saved in the memory or the file system of the mobile phone. It uses steganography to hide the IMEI, model number of the phone and the date on which the photograph is taken. When this image is forwarded via Bluetooth, the same module will get executed and the IMEI, model number and date on which image it is forwarded will be stored in the image. Objective of such an approach is to capture the original culprit or the ultimate source who captured the images or videos by backtracking and also the ones who helped in forwarding of such images and prevent such misuse of camera based mobile phones.

I. INTRODUCTION

This paper presents the J2ME application that uses steganography for hiding information in jpeg images using camera based mobile phones. A very good understanding to develop such an application is elaborated in [1].

It is necessary however to ensure that our young people are provided with sufficient guidance to make their own decision on what is appropriate to distribute via wireless networks and what the consequences could be if they allow themselves to be photographed in a situation where they could be blackmailed or embarrassed.

Normally it is not the responsibility of the service provider to monitor all the information flowing on to the network. So there is a need for a secure mechanism, to identify the owner of mobile device without his or her knowledge. Ultimately this mechanism has to be kept secret from the user community because if the user knows about such a mechanism which is included in a mobile device then it may adversely affect the business of the mobile manufacturing companies.

II. STEGANOGRAPHY

Steganography is a way or science of *concealing* information. The goal of Steganography is to hide the data from a third party [2]. Steganography allows a user to hide information within image and audio files. This form of steganography, often is used in conjunction with cryptography so that the information is doubly protected; first it is encrypted and then hidden so that an adversary has to first find the information (an often difficult task in and of itself) and *then* decrypt it.

The following formula provides a very generic description of the process of the steganography:

cover_medium + hidden_data + stego_key = stego_medium

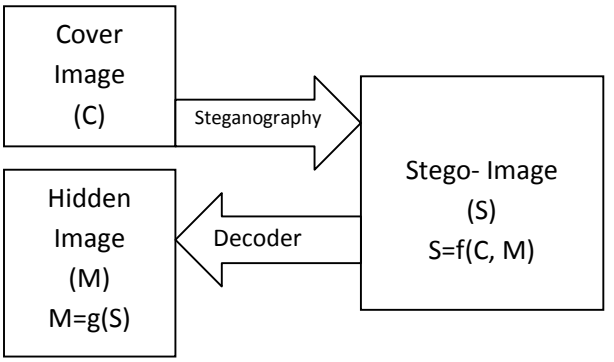

Fig. 1 Block Diagram of Stego System

In this context, the *cover_medium* is the file in which we will hide the *hidden_data*, which may also be encrypted using the *stego_key*. The resultant file is the *stego_medium* (which will, of course be the same type of file as the cover_medium). The cover_medium (and, thus, the stego_medium) are typically image, audio or video files. Figure 1 shows the basic idea about the steganography system.

The basic and fundamental requirement of any steganography system is undetectability. The hidden message should not be detected by any person considering the limited perception capability of the human visual system (HVS). Thus two aspects are usually addressed.

1. Embedding process should not degrade the image quality, that is, the difference between the stego-image and original image should be imperceptible to human eye.

2. Stego-image and original image should appear identical and also the statistics of the medium must remain unchanged [3,10].

III. JPEG

JPEG is the most common image format used by digital cameras and other photographic image capturing devices; it is also the most common format for storing and transmitting photographic images on the World Wide Web. So, we have selected JPEG as the steganography medium in the overall design.

Some methods of steganography are as under.

1. LSB (Least Significant Bit). Further information in [5, 7, 8].
2. Transformation based schemes. Several techniques for this scheme is mentioned in [3, 7, 8].

A major advantage of LSB algorithm is that it is quick and easy. But Here, We are using JPEG images for steganography. So, we can't use LSB technique to hide the text, as JPEG do the lossy compression and hence the stored information is likely to be lost.

Whereas using transformation techniques like Discrete Cosine Transform (DCT) and Discrete Wavelet Transform (DWT), they take a large amount of time to embed and the embedding capacity is also less. There are number of other ways in which embedding can be carried out like redundant pattern encoding [8], spread spectrum method [7] etc. But, these transformation based techniques require large amount of memory which is unsuitable for mobile phones as it contains limited amount of memory.

Here, we have used COMM field of jpeg image to store the data. Because comment field cannot be reflected in image data it preserves the image data as well as data which we want to hide. Also, this preserves the above mentioned two aspects.

The markers for the COM are 0xff and 0xfe and the payload is also of variable size. A detailed information about all the markers of JPEG image is shown in Figure 2.

Short name	Bytes	Payload	Name
SOI	0xFF, 0xD8	*none*	Start Of Image
SOF0	0xFF, 0xC0	*variable size*	Start Of Frame (Baseline DCT)
SOF2	0xFF, 0xC2	*variable size*	Start Of Frame (Progressive DCT)
DHT	0xFF, 0xC4	*variable size*	Define Huffman Table(s)
DQT	0xFF, 0xDB	*variable size*	Define Quantization Table(s)
DRI	0xFF, 0xDD	2 bytes	Define Restart Interval
SOS	0xFF, 0xDA	*variable size*	Start Of Scan
RST*n*	0xFF, 0xD0 ... 0xD7	*none*	Restart
APP*n*	0xFF, 0xE*n*	*variable size*	Application-specific
COM	0xFF, 0xFE	*variable size*	Comment
EOI	0xFF, 0xD9	*none*	End Of Image

Fig 2. JPEG Markers

III. EMBEDDING AND EXTRACTING PROCEDURE

Figure 3 shows the basic idea of embedding and extracting procedure. The first step is to add or find comment field in image byte array, which is preprocessing stage. The data is then encrypted and embedded in image byte array, and henceforth we get the Stego-Image. Decoding process does exactly the same in reverse to find the hidden information.

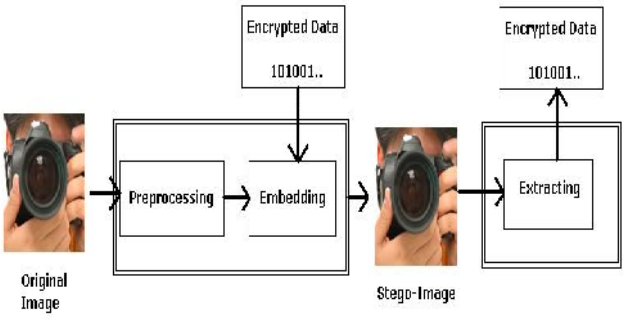

Fig 3. Embedding Procedure

Comment Field Start (0xFFFE)	Total No. of Entries	Entry 1	Entry 2	.....	Entry - n

Structure of data storage for all entries

Total Length of Entry	Length of IMEI	IMEI \O.	Length of Model Name	Model Name	Length of Date & Time	Date & Time
1	1	15	1	1-20	1	28

Structure of particular entry

Fig 4 Structure of embedded data

Figure 4 shows the structure of data to be stored in image. The count is stored immediately after the comment field starter and the structure of each entry is also shown in the Figure 4 indicating the total length of the entry, length of IMEI, IMEI Number, length of model name, Model name, length of date and time and actual date and time for the images captured.

IV. MOBILE MEDIA API

The Mobile Media API (MMAPI) is an API specification for the Java ME platform CDC (Connected Device Configuration) and CLDC (Connected Limited Device Configuration) devices such as mobile phones.

Depending on how it's implemented, the APIs allow applications to play and record sounds and video, and to capture still images.

MMAPI was developed under the Java Community Process as JSR 135 (Java Specification Request).

MMAPI includes support for a camera, with a special locator capture://video used to create its Player.

An application can use the VideoControl to display a viewfinder on the screen, then take a picture using VideoControl.getSnapshot(String imageType).

You can use the imageType parameter to select any other supported format, and query the system property video.snapshot.encodings to find out what formats are supported. [4]

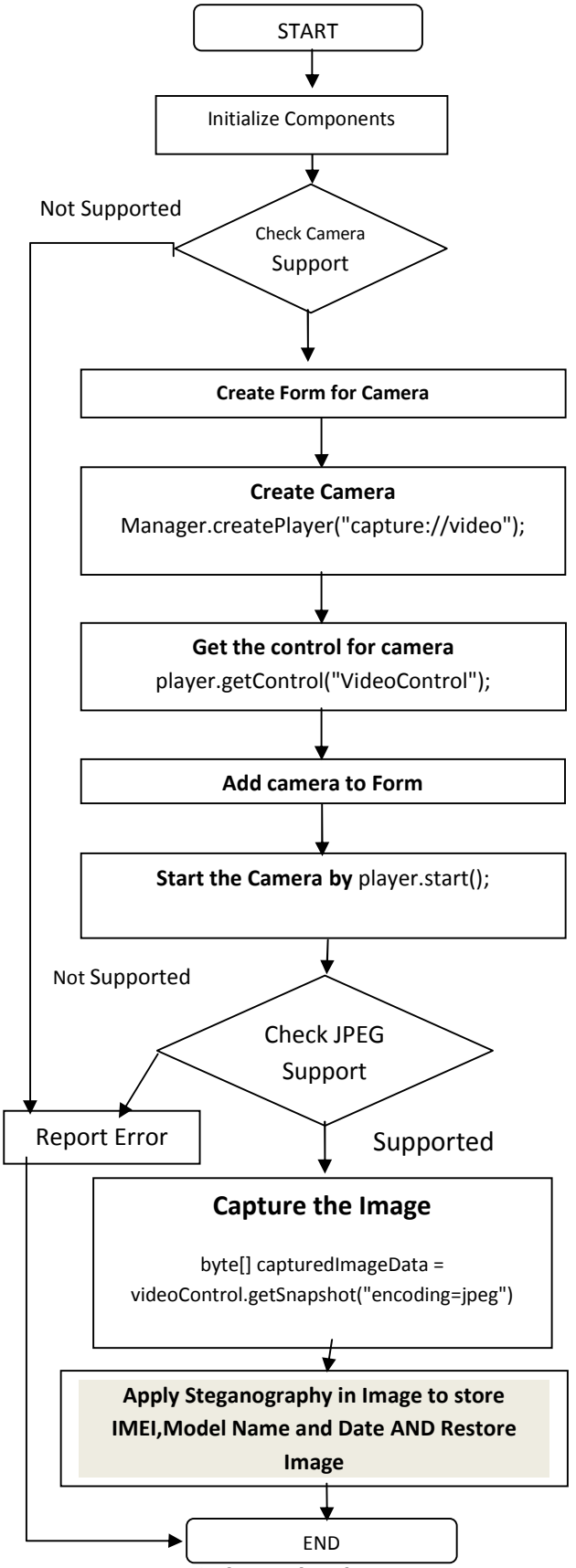

Fig 5. Application Flow Chart

Key Functions[4][6]:

1. Create Player:

   player = Manager.createPlayer("capture://video");

   player =Manager.createPlayer(“capture://image”);

2. getControl

   videoControl = (VideoControl) (player.getControl("VideoControl"));

3. getSnapShot to get the captured image

   byte[ ] jpgImage=videoControl.getSnapshot(null);

4. Read IMEI No.

   System.getProperty(“IMEI”);

5. Read Model name

   System.getProperty(“microedition.platform”);

V. FLOWCHART

Flow chart of the complete procedure involved in our design is shown in Figure 5.

VI. IMPLEMENTATION SCREEN

Figure 6 to Figure 8 shows step by step procedure for mobile application “camera” running on mobile phone “Samsung *S3650* Corby” and Figure 9 to Figure 12 shows the step by step procedure of decoder for extracting IMEI and Model name of the mobile.

This design module is tested on various mobile phones like Nokia E63,Sony Ericsson K810i and it mostly support all mobile phones which allows to read IMEI number using J2ME.

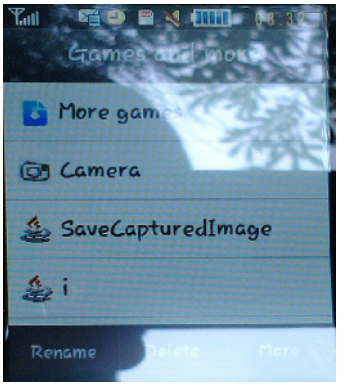

Fig. 6 “Camera” our application in mobile phone

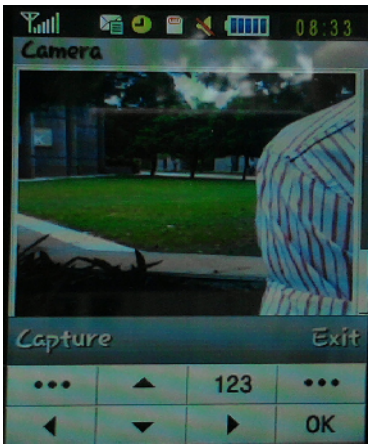

Fig 7. Application running on mobile phone

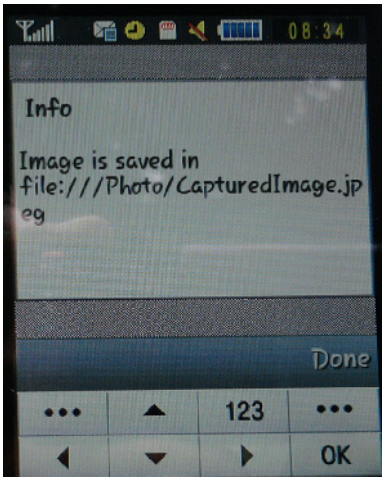

Fig 8. Stego image saved in mobile phone

User interface for the decoder is as shown below.

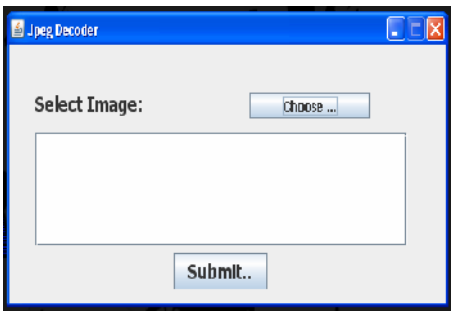

Fig 9. Step-1 click choose button to select the image

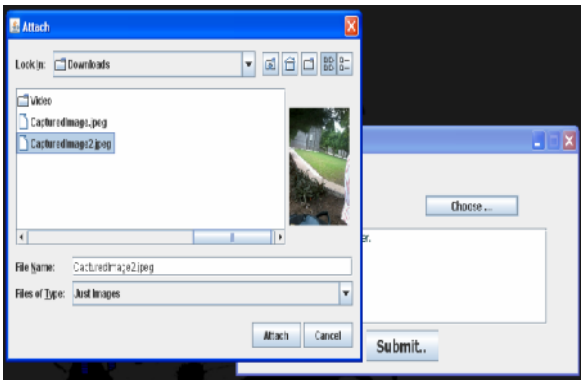

Fig 10. Step-2 selecting stego Image

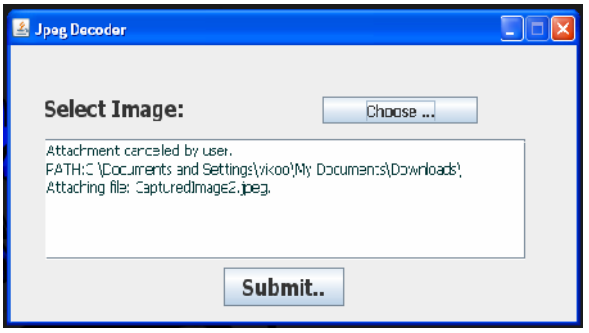

Figure 11. Step-3 Image attached and click "Submit" button to extract the IMEI Number and Model Name of the phone.

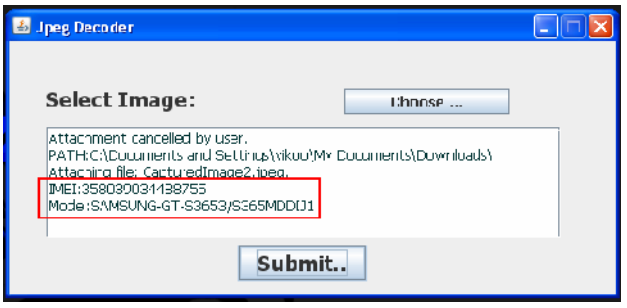

Fig 12. Step-4 Extracted IMEI and Model Name from Image

VII. CONCLUSION

The art of hiding information, if used in the positive way could help in the recognition of the criminals. With the newer and newer technology coming up in the market, misuse of all these devices is also happening in quantum. The authors have successfully implemented the paper[1] which could be a real utility for the forensic investigating authorities to solve the problems of broadcasting of nude photographs. Authors have tested the approach to see that multiple level of information is added successfully. And this information is used on the decoder side to backtrack and catch hold of the original source who has initiated this forwarding practice. Our future work will focus on video based information hiding in mobile phone and usage of blue tooth technology for the same while forwarding.

VIII.ACKNOWLEDGEMENT

We would like to thank Prof. S. N. Pradhan, Prof. D. J. Patel and Dr. K. Kotecha of NIRMA UNIVERSITY for providing continuous support and inspiration.

IX. REFERENCES

[1] Samir B. Patel, "Proposed secure mchanismfor identification of ownership of undressed photographs captured using camera based mobile phones" of the 2nd IEEE International conferenceon Digital Information Management, pp 442-447, 28-31, October 2007.

[2] Steganography: Hiding Data Within Data, Gary C. Kessler, http://www.garykessler.net/library/steganography.html.

[3] Secure Error-Free Steganography for JPEG Images, by Yeuan-Kuen Lee and Ling-Hwei Chen

[4] J2ME Mobile Media API (MMAPI- JSR-135)overview, http://developers.sun.com/mobility/midp/articles/mmapioverview/

[5] Samir B. Patel and Shrikant N. Pradhan, "An Appoach to Secure Highly Confidential documentof any size in the Corporate or Institute having Unsecured Networks" of International Journal of Computer Science and Information Security, Vol. 6, No. 2, 2009.

[6] MIDP: System Properties v1.2 (http://www.forum.nokia.com/info/sw.nokia.com/id/37086440-dcce-4fb4-aa3e-8d8c16d62b33/MIDP_System_Properties_v1_2_en.zip.html)

[7] Multimedia Security: Steganography and Digital Watermarking Techniques for Protection of Intellectual Property by Chun-Shien Lu, Idea publishing.

[8] Techniques and Applications of Digital Watermarking and Content Protection by Arnold, Michael Schmucker, Martin Wolthusen, Stephen D. , Artech House.

[9] Digital Watermarking for Digital Media by Seitz, Juergen , Information Science Publishing

[10] Information Hiding: Steganography and Watermarking Attacks and Countermeasures by Neil F. Johnson, Zoran Duric and Sushil Jajodia , Kluwer Academic Publishers.